# THE SECURITY STANDARD™

## Securing the Enterprise from a Dangerous Cyberworld

**September 19-20, 2011** • Marriott Brooklyn Bridge, New York City

Produced by

CSO

# The New Norm: A Resilient Defense – The Angelina Jolie (Lara Croft) Defense

**Jerry Archer, CISSP**

Senior Vice President and CSO

*Sallie Mae*

# The New Norm: A Resilient Defense

**Implementing an Angelina Jolie (*Lara Croft: Tomb Raider*) Defense:**

**Defending Your Enterprise in the Face of Advanced Persistent Threats and Adversaries with Significant Technical Means**

**Jerry L. Archer, SVP & CSO Sallie Mae**

# Expansion of Threat Vectors
# Reach & Range

- Advanced Persistent Threats (APTs) are reality
- Blended Threats – cross-channel, cross-domain, cross-functional
- Adversaries have significant technical means funded by cyber-crime profits and development of nation-state capability
  - Rise in Day-O and targeted attacks
  - STUXNET
- Patchwork defense characterizes current security
- Current defense obliterated by growth in technology and vulnerabilities
  - Cloud computing
  - Rich Internet Applications (RIAs)
  - Mash-ups
- Third party transparency is a major issue as third party risk continues to increase
- Compliance burden is dramatically increasing and is, generally, not accretive to improving the security posture
- Resource constraints continually challenge security program sustainability

# Defense-in-Depth Necessary but Not Sufficient

- Highly agile adversaries quickly exploit vulnerabilities
- Day-0 vulnerabilities abound and immune to signature-based defense
- Force multipliers on the order of 10,000 to 1
  - Boundary defense becomes very expensive and impractical against well-funded cyber-criminals and nation-states
- APTs complicated to detect or block
  - Blended attacks are designed to be stealthy
  - Patchwork of non-integrated defenses make it difficult to detect subtleties of attacks

When you get to a fork in the road take it.

*-- Yogi Berra*

# CHANGING TRAJECTORY

# Resilient Defense

- Identify and minimize likely targets and threats
  - Attack agility is significantly diminished when the objective is fixed or limited
- Interplay between inbound penetration and outbound exfilitration create increased visibility and thus detection opportunities
- Limiting criminal objectives means:
  - Defense becomes much more tractable
  - Well defined and can be rationalized/prioritized
  - Defense resources focused on threats which are economically feasible
- Integrating defense and intelligence create game-changer

Priorities: Detect, Deflect, Deter, Defend

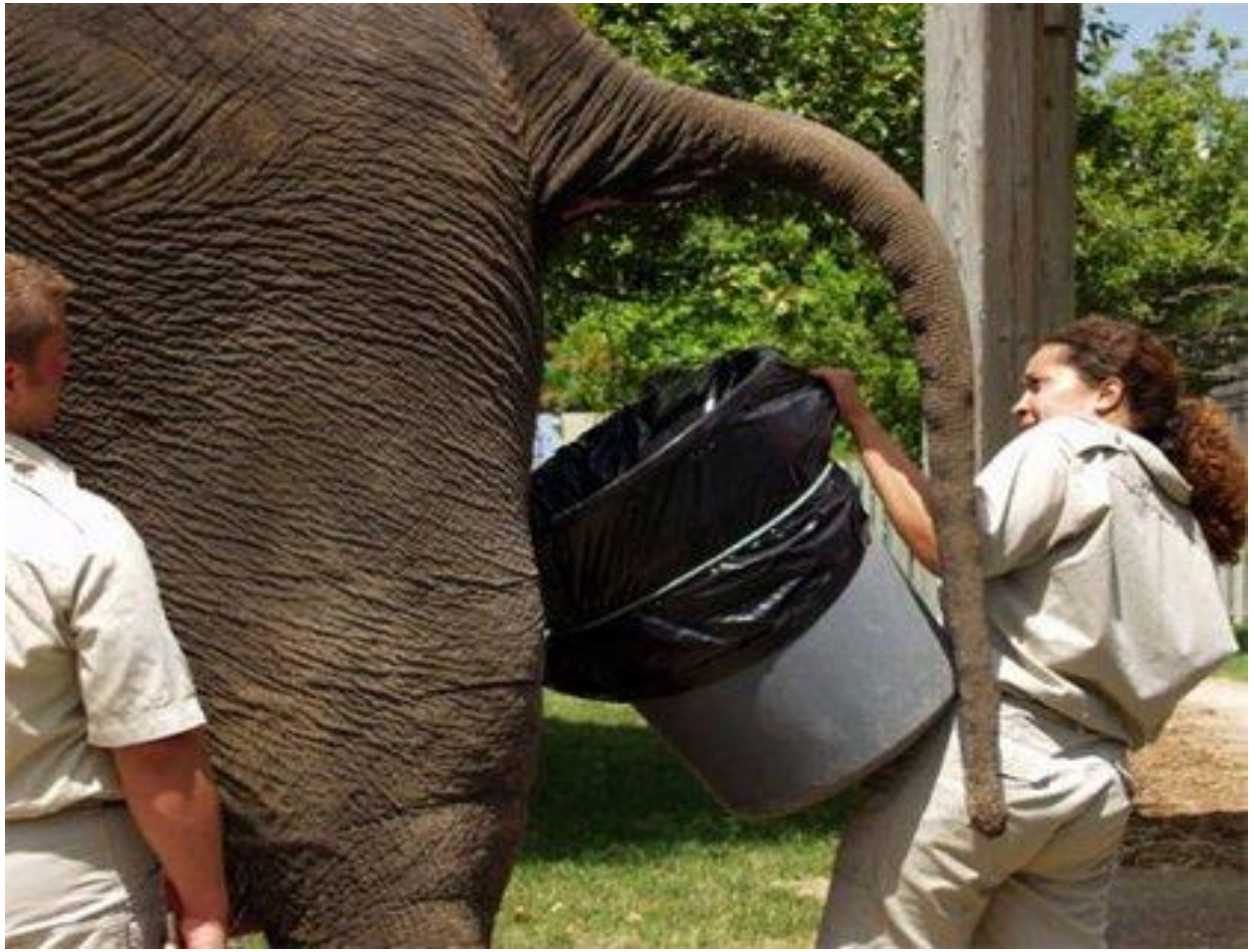
# Implementing a Resilient Defense

- Key drivers:
  - **Treat the inside like the outside**
  - **Inbound detection and prevention**
  - **Outbound detection and prevention**
  - **Choke points – compartmentalization**
- Reducing the threat plane
- Aggressive patching
- Anomaly detection
- Robust application security
- Rapid and effective incident response
- Holistic benchmarking and testing

# Steps to Successful Implementation

- Aggregate
  - Holistic security can only be achieved when it is integrated
- Automate
  - Reduce compliance burdens
  - Eliminate significant amount of first level support
  - Reduce false positives
- Arbitrage Security - RAROC
- Accelerate – processes, reaction time, change, diversity

# Failure is a bad/smelly outcome



I wish I had an answer to that because I'm tired of answering that question. -- *Yogi Berra*

# Thank You!

**Jerry L. Archer, SVP & CSO Sallie Mae**

# THE SECURITY STANDARD™

## Securing the Enterprise from a Dangerous Cyberworld

**September 19-20, 2011** • Marriott Brooklyn Bridge, New York City

Produced by

CSO